FOR PROFESSIONAL ADVISERS ONLY

REGULATORY CHANGES

MiFID II AND GDPR

As if financial advisers don't have enough to be getting on with, there has been big regulatory changes. MiFID II, the most ambitious and challenging set of reforms to affect the financial services industry for some time, took effect on 3 January 2018, and the European General Data Protection Regulation (GDPR) took effect on 25 May 2018, replacing the UK Data Protection Act 1998 (DPA).

MIFID II

Under MiFID II, financial firms such as Quilter Cheviot have brought in systems and processes to deal with the new regulation. Even with our best efforts, however, we are still working on 'grey' areas which are creating confusion.

The legislation's high level goals are:

- Increased transparency of markets
- More structured trading marketplaces
- Lower-cost market data
- Improved best execution
- Orderly trading behaviour within markets
- Costs of trading and investing made more explicit

Some of the detailed requirements have had little direct impact on your clients, for example more detailed transaction reporting and phone recording. Others, such as reporting on cost and charges and reporting a 10% fall in the value of a portfolio, have been very visible to your client and have undoubtedly affected how you initiate client relationships and your ongoing communication with them.

To help you navigate this changing landscape, we have detailed below the eight most significant changes you should be mindful of as a financial adviser.

1 NOTIFICATION OF A 10% FALL

On the face of it, the MiFID II requirement for clients to be informed when their portfolio falls 10% or more since their last report seems simple. When you consider this in a detailed way, however, a number of challenges arise. For clients of Quilter Cheviot using our nominee service, we have the responsibility to send this notification directly to the client but, as this has to be done within 24 hours, the logistics have been challenging. We do this primarily by email but also have a paper back-up. For clients affected, you should not have to take any action and we deal with this obligation. However, it is more confusing with a platform, where you need to be clear whether the platform or you should be providing this communication to the end client and how you should distribute it.

There is also a confused path of communication where financial advisers have set up their clients with a discretionary fund manager (DFM) as 'an agent of the end client'. In these cases, the DFM's obligation is to notify the financial adviser only and not the end client. This leaves the adviser to comply with this obligation.

Quilter Cheviot facilitated some of the largest peer group meetings, including other DFM firms, representatives from platforms and IFA partners with the aim of building consensus and addressing gaps in the chain, to avoid the potential of 'sleepwalking' into MiFID II.

We also thought it is helpful to show you how often the '10% fall notification' have come into effect over the last 20 years. As you see in the chart below, this have occurred a total of eight times since the beginning of 1998.

WHAT DO ADVISORS NEED TO DO?

- If you have set up your clients on the basis of 'agent as client', you will need to be sure that you understand this obligation and the implication to your business.
- Your firm may be classified by a DFM as a 'professional client'. This will mean that you need to have the specific controls and oversight to ensure your retail clients are not exposed to the same levels of risk and lower level of disclosure that applies to a professional client. You must also have the capacity and the expertise to meet your responsibilities.
- As a 'professional client', you also have to consider that if promotion of a financial instrument to a retail client has not been permitted, then your decision to purchase it on behalf of the retail client should be 'supported by detailed and robust justification of their assessment of suitability'.
- If you are acting as a 'professional client', your Professional Indemnity insurance will need to cover you for this arrangement.
- A DFM only has the obligation to notify you of a 10% fall in your client's portfolio, you therefore must have the means of notifying the end client of the fall in their portfolio or complex investment within 24 hours.

2 PROPOSAL INFORMATION AND COST AND CHARGES BREAKDOWN

Under MiFID II, a significant change is that clients must receive a breakdown of all proposed costs and associated charges related to investment or ancillary services and financial instruments, ahead of making an investment.

Quilter Cheviot can already provide the total account cost for our service, and this has been adapted to include stamp duty and investment trust costs to meet the MiFID rules for 'ex-ante cost and charge'. These are in our new Investment Proposal Document together with the other information and regulatory disclosures that we need to provide 'in good time and before commencement of the service'. The cost and charges show a breakdown between the elements that make up the costs, such as our fee, VAT, total underlying fund cost and charges, stamp duty and transaction costs. You should be able to use this data to provide an overall cost with the inclusion of your adviser charge.

For any other investments you are recommending to your clients, you should provide a breakdown of the proposed costs and charges. For those recommending a basket of mutual funds that they have selected themselves, this may require a significant amount of effort.

Remember, this information should allow the client to understand the cumulative effect of costs and charges on the return of the investment. This information should be provided at the point of sale, and also – if applicable – on a post-transaction basis.

3 REPORTING AND FEE DISCLOSURE

The MiFID II rules taking effect since January 2018 require your clients to receive quarterly valuations, transaction reports and performance updates instead of biannually. Quilter Cheviot is issuing quarterly reports which include include costs and associated charges related to the investments that we manage. The new MiFID II rules require clients to be provided with an aggregated cost disclosure (including all adviser and investment product charges) on an ongoing actual basis and to provide the clients with a full breakdown on request.

You should be able to use our figures for the cost of the service that we provide and add these to your adviser charge and 'wrapper' costs. We can provide a breakdown between the cost elements involved and an 'effect of cost' disclosure.

Again, this is additional work for you as an adviser, which will be particularly onerous if you are selecting a number of funds for your client.

4 TRANSACTION REPORTING

As part of the global push by regulators to reduce market abuse, MiFID II require us to use unique codes to identify and track anyone associated with financial transactions on markets. For an individual, we need a 'Natural Person Identifier' (NPI). The NPI code is based on the person's nationality and a specific set of identifiers. For UK nationals, the NPI should be derived from a person's National Insurance number. We also require an individual's first and last name, as well as date of birth. For other nationalities, we also require details such as a passport number, or a tax identifier, together with name and country of residence. Purchases and redemptions of unit trusts and OEICs are not market transactions and so do not need to be reported, however transactions of ETF, ETC and investment trusts will fall into scope.

5 LEGAL ENTITY IDENTIFIER LEI

For entities such as trusts, corporates, charities as well as IFA firms that are actively involved in making investment decisions in market instruments, we need a Legal Entity Identifier (LEI). MiFID firms are required to quote the LEI on almost every security transaction we undertake on behalf of clients. Without an LEI, the firm is not permitted to deal or transact on stock markets. LEIs are issued by a central organisation such as the London Stock Exchange, and there is a cost to obtain and maintain one.

Many financial adviser firms do not require an LEI, as they are not actively involved in making investment decisions in market instruments covered by MiFID II. Although trading in mutual funds does not count as 'financial transactions on markets', giving instructions for purchasing or selling ETFs, ETCs or investment trusts is in scope of transaction reporting, and an LEI will be required for your firm as well as either the LEI or NPI of the underlying client.

For clients that require LEIs, we have been writing to existing clients for their permission to apply, and offering the service to maintain the LEI, or to request that they provide us with their LEI if they are obtaining it directly.

6 VOICE RECORDING

Voice recording was proposed by the FCA for retail financial advisers. However, this was receded somewhat as the regulator conceded that a full taping obligation may not always be proportionate. Financial advisers can comply with the 'at least analogous' requirement by either taping all relevant conversations or taking a written note of all relevant conversations.

7 TARGET MARKET NOTIFICATION AND REPORTING

All financial products (PRIPS – Packaged Retail Investment Products Initiative) should have a defined target market, and the manufacturers of these products need to obtain information back from the distributors of any sales outside the defined target market. For clients using our service, we have been doing this reporting, but if you are distributing funds directly, this is an additional reporting burden on you.

8 ...AND ANOTHER REMINDER

If you have clients who established their accounts before December 2012, where you are still taking a share of our fee rather than adviser charging, we would encourage you to move these onto adviser charging as soon as practically possible.

There is a lot for financial advisers to deal with and Quilter Cheviot is committed to helping the industry prepare for these changes. Should you have any questions or feel that you would like to discuss your requirements further, please contact your respective Quilter Cheviot Regional Development Manager.

Alternatively simply call us on **020 7150 4005** or email us at enquiries@quiltercheviot.com

General Data Protection Regulation

The GDPR has been designed to harmonise data privacy laws across Europe, to protect and empower all EU citizens' data privacy and to reshape the way organisations across the region approach data privacy. However, you should already have met the bulk of the GDPR rules, if you are already subject to and comply with the Data Protection Act (DPA).

Though very similar to the DPA, the GDPR has enhanced the rules in some ways and has introduced some new elements too. Arguably the biggest change to the regulatory landscape of data privacy has come with the extended jurisdiction of the GDPR, as it applies to all companies processing the personal data of EU residents, regardless of whether the processing takes place in the EU or not. Another change is that GDPR extends to manual filing systems as well as automated personal data. Personal data that has been anonymised also comes under the GDPR, depending on how difficult it is to attribute the pseudonym to a particular individual.

LAWFUL BASIS

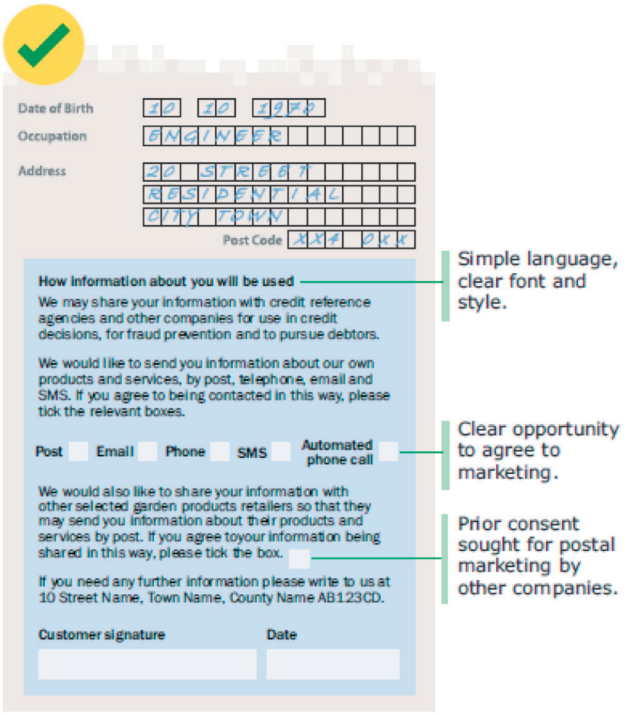
Under the GDPR, you must provide a lawful basis before you can process personal data, and this affects an individual's rights. The GDPR has created some new rights for individuals and has strengthened some of the rights that currently existed under the DPA:

- The right to be informed
- The right of access to personal information
- The right to rectification if inaccurate or incomplete
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

PRIVACY NOTICE

Privacy notices are data sharing agreements — written, electronic or oral — to be used when information is being bought, sold or rented. The GDPR requires that you take 'appropriate measures' to provide privacy information to your clients, stating clearly how you propose to use their data. Failure to obtain consent, or to check what permissions apply, may cause a breach of the code. The privacy notice must use language that is clear, concise and transparent, with the explicit requirement that it take account of the level of comprehension of the age groups involved — including children — and tailor the notices accordingly.

EXAMPLE OF A PRIVACY NOTICE



Source: Information Commissioner's Office (www.ioc.org.uk), licensed under Open Government Licence. For illustration purposes only, not to be used as templates.

All privacy notices should include the basics of who you are, what you intend doing with the data and with whom you will be sharing that data. Further notifications should also be made wherever you think the client may not be aware of the uses to which you want to put their data, or where you think that not telling people will make the processing of that data unfair. For example, you will need to gain and record your clients' consent if you intend using their personal data for research. In this case, you should offer the client an opportunity to give their consent, which they would do by ticking opt-in boxes on the appropriate form.

OPT-IN, OPT-OUT

Any opt-in requests need to be displayed clearly and prominently, giving clients sufficient information to make a choice. If you want to make multiple uses of the data, then you must ensure that your clients can give their consent for each use individually. A single, blanket opt-in would not meet requirements. Best practice is to list all the different uses, each with its own unticked opt-in box to invite the person to confirm their agreement by ticking. This is also good practice if you want your clients to receive any direct marketing or other communications such as newsletters.

The practice of using pre-ticked opt-in boxes relies on the user to untick the box if they want to object. Effectively, a pre-ticked opt-in box only assumes consent, rather than being a positive, informed choice by the user, and will not be enough to demonstrate full consent — it is quite possible that the user may simply have not seen the box.

DATA BREACH

The key responsibility for you as a financial adviser is that any notifiable data breach will need to be reported to the relevant supervisory body within 72 hours of the breach being detected, where feasible. The 'notifiable' data breach refers to any loss of data that could expose clients to identity theft, or otherwise jeopardise their rights and freedoms.

SECURITY

You will be held responsible for keeping all your client data secure, protecting it against unauthorised or unlawful processing, accidental loss, destruction or damage, even when outside the office, for example when visiting clients. Any documentation left in the car should be locked up in the boot. Firms have to set up systems to protect data, including communications sent externally, and be able to demonstrate their compliance with these principles.

Firms are advised to have strong systems in place (whether software or procedural), so that in the event of a data breach they will be able to conduct an audit and, critically, be able to show how they had carried out their responsibilities towards their clients. Failure to do so may result in harsh penalties, with fines of up to €20 million, or 4% of turnover.

Work on GDPR is ongoing, and a number of questions need to be resolved. The industry is lobbying for any fines for a data breach to be applied proportionately, as small IFA firms will most likely be unable to pay large fines. Greater clarity is being sought about whether aspects of the GDPR will come within the jurisdiction of the Financial Conduct Authority or the Information Commissioner's Office (ICO), the UK government-sponsored regulatory body responsible for upholding citizens' information rights.

THE ICO HAS SET OUT 12 STEPS THAT YOU NEED TO TAKE:

1 Awareness - Make sure that decision makers and key people in your organisation are aware of the GDPR changes, and appreciate the impact they are likely to have.

2 Information you hold - Document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.

3 Communicating privacy information - Review your current privacy notices and put a plan in place for making any necessary changes required under GDPR. Use plain language. Tell them **who** you are when you request the data. Say **why** you are processing their data, **how** long it will be stored and **who** receives it.

4 Individuals' rights - Check your procedures cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format. Give people the 'right to be forgotten'. Erase their personal data if they ask, but only if it doesn't compromise freedom of expression or the ability to research.

5 Subject access requests - Update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

6 Legal basis - Look at the various types of data processing you carry out, identify your legal basis for carrying it out and document it.

7 Consent - Review how you are seeking, obtaining and recording consent and whether you need to make any changes. Ensure you get their clear consent to process the data.

8 Children - Start thinking now about putting systems in place to verify individuals' ages and to gather parental or guardian consent for the data processing activity.

9 Data breaches - Make sure you have the right procedures in place to detect, report and investigate a personal data breach. Inform people of data breaches if there is a serious risk to them.

10 Data protection - Familiarise yourself now with the guidance the ICO has produced on Privacy Impact Assessments, and work out how and when to implement them in your organisation. Use extra safeguards for information on health, race, sexual orientation, religion and political beliefs.

11 Data protection officers - Designate a Data Protection Officer, or someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements.

12 International - If your organisation operates internationally, you should determine which data protection supervisory authority you come under. Make legal arrangements when you transfer data to countries that have not been approved by the EU authorities.

QUILTER CHEVIOT
Senator House
85 Queen Victoria Street
London EC4V 4AB

Please contact our Marketing Department on +44 (0)20 7150 4000 or email marketing@quiltercheviot.com

quiltercheviot.com